CONSTRUCTION SECURITY PLAN
F-35 LIGHTNING II RENOVATION FRCSE

RELEASE REV 1.0
Oct 18 2024

(U) TABLE OF CONTENTS

(U) APPENDIX LIST

1.0 BASIC INFORMATION

1.1 **(U) SITE SECURITY MANAGER (SSM)**
Name: David A Steiner, SFPC, PSC, SPSC (FRCSE GSSO)
Mailing Address: P.O. Box 16, Jacksonville, FL 32212-0016

Classified email: contact the SSM
Duty Hours: 0600-1530 M-Th (0600-1430 F

(U) ASSISTANT SITE SECURITY MANAGER (ASSM):
Name: TBD (hiring action underway)
Mailing Address: P.O. Box 16, Jacksonville, FL 32212-0016
Email: TBD
Classified email: contact the SSM
Duty Hours: 0600-1530 M-Th (0600-1430 F)

1.2 (U) STATEMENT OF CONSTRUCTION PROJECT
Sections of Fleet Readiness Center Southeast (FRCSE) Building 101, will be renovated to meet current ICD 705 Tech Specs to meet multi-level classification for a stakeholder. These buildings will be support operations areas, and a centralized conference center at multiple levels.

(U) The CSP addresses the project as a whole, with main focus on the secure facility areas to be constructed.

1.3 (U) Not applicable

1.4 (U) Not applicable

1.5 LOCATION OF WORK
(U) All work will be performed onboard Naval Air Station Jacksonville, Jacksonville Florida at FRCSE Building 101.

1.6 (U) ESTIMATED START DATE
(U) 2QFY25

1.7 (U) ESTIMATED COMPLETION DATE
(U) 4QFY26

1.8 (U) HAS A RISK ASSESSMENT BEEN COMPLETED
(U) See APPENDIX E

1.9 (U) ACCREDITATION SUPPORT PLAN
(U) See APPENDIX M

1.10 (U) CONSTRUCTION SECURITY INSPECTION CHECKLIST
(U) See APPENDIX L

1.11 (U) SECURITY ADMINISTRATION

(U) The SSM and SSM Staff will maintain all administrative documents, logs, and records related to the security of this project to be included in the final accreditation package. This includes but not limited to: all administrative actions completed by the SSM Staff (observation notes, visitor logs, material submittal sheets, incident reports, photos, access control logs); requests for information (RFI's); the master access roster, and any other documents, logs, or reports produced.

1.12 (U) DOCUMENTATION CHECKLIST
(U) See APPENDIX O for accreditation documents and checklist

2.0 (U) PURPOSE AND ORGANIZATION

2.1 (U) PURPOSE OF THE CONSTRUCTION SECURITY PLAN

(U) The purpose of the Construction Security Plan (CSP) is to identify the security requirements, procedures, and standards that will be implemented throughout the Secured Facility construction project, to deter and detect unauthorized access to, and reduce the risk of security hazards at the construction site and any protected storage areas, and protect the end user mission and US national security. This CSP will specifically address Construction Site Security (CSS) in its entirety.

(U) The CSP will be incorporated as part of the overall construction contract. No changes, modifications, nor reductions of the requirements outlined in this document are authorized without Accreditation Official (SAO) approval. For the duration of the project all personnel involved will adhere to the most current version of the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec for ICD/ICS 705. All questions about this CSP shall be directed to the SSM.

(U) This Construction Security Plan is **a living document** and serves as the primary reference for security policies and procedures to be employed at the construction site until completion of the project. The SSM may make minor modifications, as approved by the SAO, to these requirements that do not increase risk, as necessitated by changing local conditions i.e. weather, civil unrest, natural disasters, or base mandated emergency action plan implementation.

(U) The CSP applies equally to anyone, and everyone associated with this construction project. This includes all persons who will or may, regardless of reason, access the Project Construction Site, access Project Documentation (e.g. blueprints/construction documentation) even if they will not access the SCS, attend project meetings, and/or obtain project specific information.

(U) The success of this project is dependent on the mutual collaboration of contractors and US Government Personnel. The US Government, as the tenant, has incorporated security requirements into the Request for Proposal (RFP) and this CSP to aid in the proper execution of the project as it pertains to security requirements.

(U) Upon approval of this CSP by the SAO, an Unclassified (U) version of the CSP will be created and sent to NAVFAC PM/CSC. NAVFAC PM/CSC shall incorporate the CSP requirements in the construction documents to ensure costs are included in the contractor proposals and during contract performance.

(U) Any Controlled Unclassified Information (CUI) or Classified appendices or annexes will be distributed to "need to know" personnel (cleared person) by the SSM upon approval from the SAO.

(U) Classified appendices shall only be used in spaces cleared to the level of the classification of the document. Classified appendices will be maintained and controlled by the U.S. Government and stored in a locked GSA Security Container whenever the documents are not in active use under the direct physical control of a cleared person.

(U) A list of all personnel and security clearance Access levels will be verified and kept by the SSM to be incorporated into the final Accreditation package. Requests for classified information shall be made to the SSM for the duration of the project. The SSM will have not less than five (5) working days to review all requests unless an urgent matter or work stoppage occurs. Urgent or "Work Stop" matters will be reviewed as soon as possible and the SSM will have a goal of review within one-working-day of the request.

(U) This CSP will apply to all areas of the construction site. The policies and directives contained in the CSP are considered the minimum standard to be applied to this project. These requirements may be modified, or additional safeguards may be added, at the discretion of the SSM, with concurrence of the SAO, if necessitated by unusual or changing local conditions. Changes to this CSP must be submitted to the SAO via Fleet Readiness Center Southeast (FRCSE) and Commander, Fleet Readiness Centers. The NAVFAC PM/CSC will be notified of all changes submitted. Written agreement by all signatories of the CSP is required to effect any change. Contractual change considerations because of any CSP change must be approved by the assigned NAVFAC PM.

(U) An UNCLASSIFIED version of this CSP will be included in the solicitation package to ensure that all construction bidders understand the security requirements for this project and ensuring, the requirements contained within the most current version of the ICD/ICS 705 Tech Spec and this CSP are implemented and advising the SAO of compliance or variances. A full CUI version may be provided to construction bidders that complete a Non-Disclosure Agreement, Appendix A.

(U) Construction and design of secure facilities shall also be compliant with Fire code and National Fire Protection Association 1, Life safety code NFPA 101, The Americans with Disabilities Act 28 CFR Part 36, and the Uniform Federal Accessibilities Standard where applicable.

2.2 (U) ORGANIZATION CONTACT LIST

(U) The Site Security Manager (SSM) provided in section 1.1 is a U.S. Government supplied position that will be the U.S. Government's representative to ensure all security requirements of the CSP are met. The SSM is responsible for the oversight of project security requirements and security personnel, with responsibility for coordinating all site-specific security aspects of the project. Contact to the SSM shall be in writing for all questions and responses regarding the CSP and associated actions and activities.

(U) NAVAL FACILITIES (NAVFAC) PROJECT MANAGER/CONSTRUCTION SITE COORDINATOR(CSC):

Name: Dominic Drdla

Mailing Address: NAVFAC SE, Box 30, Jacksonville, FL 32212-0030
Commercial Phone: 904-542-6918
DSN: 312-942-6918

(U) The NAVFAC PM/CSC is a U.S. Government supplied position that will be the U.S. Government's representative for management of the construction process, schedule, and assisting the Contractor in resolving any problems that may arise.

2.3 (U) PROJECT DESCRIPTION

(U) Construction project will construct a new Secure Facility located at Naval Air Station Jacksonville. This project is located inside of building 101, which is a complex two-story structure within a Level Two Restricted Area as defined by the SECNAVINST 5500.35, Navy Physical Security Program. The new facility will establish the capability to house sensitive material and workstations to allow operations that require enhanced-security measures.

(U) The Secure Fixed Facility will be designed to Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.5.1, of 26 July 2021 (IC Tech Spec-for ICD/ICS 705), or the current issued Version, including exterior wall systems, doors, and windows.

(U) The following codes, as needed, will apply to this project:

- Intelligence Community (IC) Tech Spec-for ICD/ICS 705 version 1.5.1, 26 July 2021
- International Building Code (IBC), 2021 edition
- ASCE 7-05-Minimum Design Loads for Buildings and Other Structures
- UFC 1-200-01-General Building Requirements, with Change 2, 06 June 2023
- FC 1-300-09N-Design Procedures, with Change 6, 09 July 2021
- UFC 3-301-01-Structural Engineering, with Change 1, 10 October 2023
- UFC 4-010-01-DoD Minimum Antiterrorism Standards for Buildings, with Change 2, 30 July 2022
- UFC 4-010-05-SCIF/Secure Facility Planning, Design, and Construction, 26 May 2023
- UFC 4-010-06 Cybersecurity of Facility-Related Control Systems, 10 October 2023
- UFC 4-021-01 Design and O&M: Mass Notification Systems, with Change 1, 01 January 2010
- UFC 4-021-02 Electronic Security Systems, with Change 1, 11 September 2019
- UFC 4-022-01 Security Engineering: Entry Control Facilities / Access Control Points, 27 July 2017
- UFC 4-022-03 Security Fences and Gates, 10 January 2013
- CNSSAM TEMPEST/1-13, RED/BLACK Installation Guide, 17 January 2014

2.4 (U) LOCATION

(U) The renovation will be located within the FRCSE headquarters building, 101 Wasp Street, NAS Jacksonville, located in Jacksonville, Florida.

2.5 (U) TIMELINE

- RFP proposals due: FY25 (pending)
- Estimated BOD: FY25 (pending)
- Construction contract award: FY25 (pending)
- Estimated Construction Phase (start): FY25 (pending)
- Estimated Fit-Up Phase (start): FY26 (pending)
- Estimated Completion Date: FY26 (pending)

3.0 (U) PROJECT MANAGEMENT

3.1 (U) REFERENCES

(U) The construction site security measures and fixed facility administration will be implemented in accordance with the following:

- DoDM 5200.01 Volume 3, with Change 3, DoD Information Security Program: Protection of Classified Information, 28 July 2020
- DoDM 5200.02, with Change 1, Procedures for the DoD Personnel Security Program (PSP), 29 October 2020
- DoDD 5205.02E, with Change 2, Operations Security Program, 20 June 2012
- DoDM 5205.02, with Change 2, DoD Operations Security (OPSEC) Program Manual, 29 October 2020
- DoDM 5205.07 Volume 1, with Change 2, DoD Special Access Program (SAP) Security Manual: General Procedures, 30 September 2020
- DoDM 5205.07 Volume 2, with Change 2, Special Access Program (SAP) Security Manual: Personnel Security, 30 October 2020
- DoDM 5205.07 Volume 3, with Change 3, SAP Security Manual: Physical Security, 08 December 2020
- ICD 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation, dated 15 September 2008
- ICD 705, Sensitive Compartmented Information Facilities, dated 26 May 2010
- ICD 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities, dated 17 September 2010
- IC Tech Spec for ICD/ICS 705 Version 1.5.1, Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, IC Tech Spec for ICD/ICS 705 dated 26 July 2021
- DoD 5105.21-V2, Sensitive Compartmented Information Administrative Security Manual, dated 19 October 2012
- ICS 705-2, Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities, dated 11 February 2013
- ICD 731, Supply Chain Risk Management, dated 7 December 2013
- CNSSAM TEMPEST/ 1-13 Red/Black Installation Guidance, dated 17 January 2014
- UFC 4-010-05, Sensitive Compartmented Information Facilities Planning, Design, and Construction, dated 1 February 2013 Change 2, 16 June 2022
- UFGS 8 34 7, Sound Control Door Assemblies
- UFGS-01 14 00, Work Restrictions, dated November 2011 Change 14 – 08/22
- SECNAVINST 5500.35 Navy Physical Security Program of 22 Feb 2022
- FRCSEINST 5500.5B Physical Security Plan, 05 September 2017
- FRCSEINST 5500.14A Information, Personnel, and Industrial Security Procedures, 19 November 2018

3.2 (U) RISK ANALYSIS AND THREAT ASSESSMENT

(U) For the construction of all Fixed Facility projects, a risk analysis shall be conducted and documented utilizing a certified risk analysis process, such as “Analytical Risk Management”. The risk analysis process will be under the cognizance of the offices of primary interest, with input from major

stakeholders. The risk assessment will address any threat that poses a hazard to this activity. The hazard is predicated on foreign intelligence activities; terrorism; civil unrest; crime; war; and Acts of Nature.

(U) The CSP will employ risk mitigation measures to achieve an adequate level of protection against indicated threats during the design and construction process for the Fixed Facility. The risk management and threat assess may be refreshed periodically, and the CSP measures may be modified to bring it in line with the most current risk analysis. See Annex E: Risk Assessment.

(U) A Critical Program Information (CPI) list has been developed by the F-35 Program Office in support of Operation Security (OPSEC) in accordance with DoD Directive 5205.02E. The OPSEC plan process will identify "critical program information" related to this effort. Basic Critical Program Information is identified in Appendix B, and additional information is in the Appendix E of the F-35 LIGHTNING II Program Protection Plan (classified).

3.3 (U) SECURITY IN DEPTH

(U) The Security-in-Depth (SID) for this project has been established to protect the construction project throughout the construction lifecycle process by enhancing the probability of detecting adversary actions before the access to the Secure Facility is achieved. The SID layers are:

- (U) This construction project is on Naval Air Station Jacksonville (NAS JAX) with 24-hour access control performed by Department of Defense Police, U.S. Navy Military Police and NAS Jacksonville Auxiliary Security Forces, collectively identified in this document as Security Forces (SF) who are all U.S. citizens.
- (CUI//NF) FRCSE has a Level 2 Restricted Area controlled access compound on-board NAS JAX that is fully fenced. Electronic access control is implemented and utilized.
- (CUI//NF) FRCSE has a 24-hour non-armed civil service guard staff that perform continuous roving and random checks throughout the day and night.
- (U) Any suspicious behavior will be reported to the NAS Jacksonville SF through the Navy Region Southeast Public Safety Access Point (E-911) system and the FRCSE Command Duty Officer (CDO). Secondary notification is made to the FRCSE Security Director/Activity Security Manager (ASM). The CDO and/or ASM will provide additional notifications to the SSM, F-35 Military Director, and FRCSE Physical Security Officer.
- (CUI//NF) Following demolition of the interior of Mezzanine 7 and prior to beginning any work for the Secure Facility, the entire Mezzanine 7 area will be controlled with access only permitted from at a single entrance and check in point. This area will be restricted to only those with approved access. The entry point will be the roll up door / ramp at the Southeast corner with a check-in point manned during working hours by FRCSE civil service guard staff (or other person appointed by SSM). Outside of working hours, the Mezzanine 7 area will be locked and secured.
- (U) Once the baseline construction (walls and doors) is complete, the SSM will control access to the Secure Facility boundaries for final fit up for only those with approved access.

3.4 ADJACENCIES TO CONSIDER

Not applicable

3.5 (U) CONSTRUCTION WORKERS, OTHER PERSONNEL, AND COMPANIES

(U) All information obtained for the purpose of vetting personnel shall be protected in accordance with the Privacy Act of 1974.

(U) the SSM shall create a Master Access Roster for use on this project that will identify all persons who are approved for project area access and/or project information and separately shall identify anyone who has been denied for use on this project.

(U) All persons shall be U.S. citizens or US persons who have been positively vetted in accordance with this CSP.

(U) All contractor and sub-contractor employees participating in this project shall complete the Controlled Unclassified Information Non-disclosure Agreement contained in Appendix A.

3.5.1 (U) UNCLEARED PERSONNEL (Persons without a U.S. security clearance eligibility and current Access at the Secret or higher level.)
(U) Contractor employees requiring access to project information, material, and/or access to the project site will be required to complete a Contractor Vetting spreadsheet and endorse an Authorization for Release of Information form. Information required is listed in the table below. Original documents, or notarized document copies, may be requested for identity validation.

- Full legal name as shown on birth certificate, marriage certificate, legal change of name documents, or passport, and any aliases.
- Current residence address(es).
- Date and place (city, state/province, country) of birth.
- Information pertaining to all citizenships held.
- Social Security Number.
- Driver's License Number or State Identification Number.
- Identification of active Passports with Passport number(s).
- Inclusive dates of access required.

(U) The SSM shall notify the NAVFAC PM within 21 days when approvals or denials are made for submitted personnel. The 21-day vetting clock will not start until the SSM receives a complete and accurate submission. The SSM reserves the right to deny access pending additional details if any of the above information is not included in the submission, or the submitted information is not accurate or legible. The SSM will comply with all PII protections in accordance with U.S. Federal law and Department of Defense regulations.

(U) All persons shall be vetted by FRCSE Security prior to being authorized access to the project areas except for emergency responders responding to an emergency in the area of the project. Emergency responders include fire department, law enforcement, emergency medical and NAS Jacksonville or FRCSE civil service employees directly supporting the emergency response. The emergency response period shall be considered as over when fire department, law enforcement or emergency medical services have cleared the project area. All project area access vetting shall be accomplished in accordance with the current FRCSEINST 5500.5 and FRCSEINST 5510.14 instructions.

(U) In accordance with U.S. Government policy, the design and construction of this project shall be accomplished by U.S. companies using U.S. citizens. Proof of U.S. citizenship is required for individuals requiring access to construction site, project information, and/or project materials on the site. One of the proofs of identification listed on the U.S. Employment Verification Form, I-9, may be used. The use of E-Verify by contractors to validate employee U.S. citizenship is required (48 CFR subpart 22.18).

(U) Use of non-U.S. citizens requires prior written approval by the SAO, approval is contingent upon acceptable risk of established mitigations. These mitigations shall be documented in the CSP. The NAVFAC PM/CSC shall provide written requests for use of non-U.S. citizens to the SSM a minimum of 21 working days prior to the date of access required.

3.5.1 (U) CLEARED PERSONNEL (Persons with a U.S. security clearance eligibility and current Access at the Secret or higher level.)
(U) The Company Facility Security Officer (FSO) shall submit a single Visit Request (VR)in the Defense Information System for Security (DISS) for all employees to Security Management Office code N658865. This DISS VR will be maintained and updated by the FSO for the duration of the Companies performance on this Project. Additionally, the FSO will notify the SSM by e-mail of all modifications to the DISS VR at the time of the modification of the DISS VR. Cleared personnel not included on the DISS VR will not be permitted access to the Project information or worksite.

3.5.3 (U) STATEMENT OF AFFILIATION
(U) All contractor and sub-contractor companies participating in this project shall complete the Statement of Affiliation contained in Appendix B.

3.5.4 (U) REMOVAL FOR CAUSE
The SAO or SSM may deny access or remove any contractor or from the project site any U.S. Government employee for good reason. The Contractor or contractor employee may not be informed of the reasons for the denial without approval of the SAO.

(U) Contractors and sub-contractors shall provide Statement of Affiliation (Appendix B).

(U) All personnel submitting information shall be required to complete an acknowledgement of advisement of the Privacy Act and will be required to sign an Authority for Release of Information, both of which shall be supplied during processing. Release documents must be turned in with the submission of information identified above. Information obtained for vetting will be adjudicated by the SSM, SAO, and designated appointees who will have the final decision regarding access to the site, site information, and/or site construction material. In accordance with the Privacy Act of 1974, information obtained for adjudicative purposes will not be shared outside of elements involved in the adjudicative process. The SSM will not share the rationale for adjudicative decisions.

3.6 (U) DEFENSE BIOMETRIC IDENTIFICATION SYSTEM (DBIDS)
(U) NAVFAC is responsible for coordinating contractor access to the base. The NAVFAC PM/CSC will sponsor contractors utilizing DBIDS via the SECNAV Form 5512-1 for identity management and installation access control. Construction personnel requiring access to the project site are subject to

security vetting by the U.S. Government via electronic databases, i.e., NCIC/FBI/DBIDS/NSA. All DBIDS revocation and denial appeals will take place at the Naval Air Station Jacksonville Pass and ID (PID) Office. Naval Air Station Jacksonville may implement policies and standards of conduct beyond those provided by this project as they pertain to personnel. These policies and standards are at the sole discretion of the installation. Personnel must abide by installation policies and standards both on Naval Air Station Jacksonville, and in all instances when absent from the construction site. Violations of the installation's policies and standards will be assessed at the sole discretion of the Installation Commander and/or NAVFAC SE Commanding Officer, when not related to actions on the construction site. Grounds for a contractor employee becoming ineligible and access privileges suspended/revoked or no longer employed with the contractor must be immediately reported to the NAVFAC PM/CSC and SSM or designee for adjudication.

3.8 (U) REPORTING REQUIREMENTS

(U) Should approved employees have adverse contact with Law Enforcement following their initial provision of information for vetting, contractor must report any/all adverse information (e.g. speeding, DUI, DWI, sex offense, felony conviction, drugs, and order of arrest regardless of the offense/violation) to the Contract Security Representative or COR who will coordinate the adverse information with the NAVFAC PM/CSC, SSM, and SAO to determine immediate removal or continued access to work site, materials, and/or project information.

(U) All personnel are required to immediately report all security incidents, concerns, or suspected violations to the SAO via the SSM, NAVFAC PM/CSC, and project COR for risk determination and decision for continued access to work site, materials, and/or project information. The U.S. Government shall not be responsible for security incidents that create an impact to schedule or costs when it is determined, by the appropriate U.S. Government representative that the contractor, sub-contractor, or their employee is in error.

(U) All personnel must immediately bring safety concerns and issues to the attention of the NAVFAC PM/CSC, their supervision, or other personnel as appropriate. The CSC shall immediately notify the SSM, or designated appointee, when safe to do so. All reporting will be done in accordance with NAVFAC requirements as specified in the RFP and contract documents. Any requests for project information by the media or entities outside the project shall be referred immediately to NAVFAC PM, the SSM. All information released to the media will be released through the FRCSE or NAVFAC Public Affairs Office (PAO). Other information requests will be handled on a case-by-case basis by the FRCSE Command Operations Group.

3.9 DOCUMENT CONTROL

(U) CONTROLLED UNCLASSIFIED INFORMATION (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under E.O. 13526 or the Atomic Energy Act, as amended. CUI information may be stored in locked file cabinets, rooms, or buildings. CUI information may be left in unlocked areas when internal security measures preclude unauthorized access. CUI information will be destroyed in a manner which precludes reconstruction of the information (i.e., shredding/burn bags). See

DoD Instruction 5200.48 for additional information. Additional information and training are available at https://www.dodcui.mil

(U) The CUI marking guidance in this SCG falls under the "Defense" category with the specified subset being DoD Critical Infrastructure Security Information. Documents containing CUI will be marked "CUI" in accordance with the DoD Instruction 5200.48.

(U) For the purposes of this CSP, design information and project related documents/information will be considered as Controlled Unclassified Information (CUI) at a minimum. CUI documents and shall never be shared with anyone who does not have a validated need to know. The SSM shall confirm valid, and final, need to know if ever uncertain. Design information and project related documents/information includes, but is not limited to, the following types of information: drawings, blueprints, schematics, schedules, memorandums, sketches, meeting minutes, vendor lists, material orders and bills of lading, access rosters, and project emails. See Annex F: Critical Program Information (CPI)

(U) The Contractor shall prepare an OPSEC plan in accordance with DoD Directive 5205.02E or the current issued revision or change and FAR 4.1303-91 Operations Security (OPSEC) For On-site Contractors.

(U) The Contracting Officer (KO) shall insert procurement note H16 in solicitations and contracts when contract performance requires contractors to have intermittent and/or routine physical access to a Federally-controlled facility and/or intermittent and/or routine access to a Federally controlled information system.

(U) Prior to accessing CUI, the contractor and all sub-contractors shall complete and submit the Controlled Unclassified Information Non-Disclosure Agreement (Appendix A) (CUI NDA). The CUI NDA will be submitted to the SAO and a copy held by the SSM as part of the project records file.

(U) To the greatest extent possible, the Project documents shall not include any markings, known as "prohibited terms", identifying spaces or buildings as "Special Access Program Facility", "SAPF", "Special Compartmented Information Facility", "SCIF", "Compartmented Area", "CA", "Secure Working Area", "SWA", "Temporary Secure Working Area", or "TSWA". The term "Restricted Area" shall be used in lieu of the prohibited terms. Documents that contain the prohibited terms listed above will be closely controlled by the SSM and only provided to the Contractor if there is a 'exceptional need-to-know' requirement provided by the NAVFAC PM.

(U) All construction plans shall be marked as Controlled Unclassified Information (CUI), specifically CUI Category: DCRIT/OPSEC, Limited Dissemination Control: SP-CTI/FEDCON/NOFORN, and disseminated to only those approved to work on this project under controls identified elsewhere in this document.

(U) Under no circumstances should documents, plans, diagrams, etc. that are identified for a Special Access Program Facility (SAPF), Sensitive Compartmented Area Facility (SCIF), Compartmented Area (CA), Temporary Secure Working Area (TSWA), or similar ICD 705 facility be sent, stored, processed,

or posted on unprotected information technology systems or any Internet venue without encryption meeting Federal Information Processing Standard (FIPS) Publication 140-3. Construction documentation will only be disseminated to designated individuals with valid need to know and shall not be posted to public websites. Only US Government or Official Contractor information systems utilizing commercially available technical/information assurance controls incorporating Federal Information Processing Standard (FIPS) Publication 140-3 shall be utilized to store, safeguard and transmit/receive email, tasking's or other correspondence relating to this project. Electronic IT systems used for this Project shall have a current Authority To Operate (ATO) issued by the U.S. government or shall be approved in writing for use by the NAVFAC Chief Information Officer or their designated official. The use of private email or communications services such as Gmail, Yahoo, Hotmail, Facebook, Whatsapp, Proton Mail, non-U.S. Government Zoom or non-U.S. Government Microsoft TEAMS, or other similar commercial services that do not have an approved ATO issued by the U.S. government shall not be used to transmit any CUI or classified national security information (CNSI).

(U) Vendors/manufactures shall not be told the name of the end user, name of this project, nor that the work is classified, sensitive, or otherwise related to US National Security.

(U) During the duration of the project all drawings, blueprints, schematics, schedules, memorandums, sketches, meeting minutes, vendor lists, access rosters, and project emails when not in use and at the end of each day shall be stored in locked cabinet or room. Access to these documents shall be limited to only those persons directly associated with the project who have a validated need to know the information and have signed a non-disclosure agreement.

(U) When no longer needed, physical documents held or created by the Contractor, or any sub-contractors marked CUI, including all project document, blueprints, plans, designs, meeting minutes, and all other CUI documents shall be physically destroyed by the Prime Contractor using cross cut shredding. Only cross-cut paper shredders currently listed on the most recent National Security Agency, Central Security Service (NSA/CSS) Evaluated Product List for High Security Crosscut Paper Shredders shall be used. The Prime Contractor is responsible for procuring the cross-cut paper shredder(s) for contractor use. The Prime Contractor shall provide the PM and SSM a list of cross-cut paper shredders intended for use. A log of documents destroyed by the Contractor will be maintained and submitted to the SSM monthly, not later than the 3rd working day of the month following the month the documents were destroyed. The log will include the date of destruction, the document title, and indicate if the entire document was destroyed or page(s) and/or sheet number(s) destroyed if only portions of documents are destroyed, and the printed name of the person destroying the document(s).

(U) When required to meet U.S. Government records keeping policy, documents shall be returned to the U.S. Government office that issued the material or documents.

3.9.1 (U) PUBLIC RELEASE:

The fact that certain information is unclassified does not permit automatic public release of the information. The F-35 Lightning II Program Office is the control authority for all Public Release material. Proposed public release of unclassified information regarding any aspect of this project, shall be submitted to the F-35 Lightning II Program Office Public Affairs Office (PAO), through the FRCSE SSM

and FRCSE PAO offices, for a review with a minimum of 15 days prior to the proposed date of release. Proposed release of Controlled Unclassified Information outside of the parties directly involved with this project regarding the project shall be submitted to the FRCSE SSM for forwarding to the F-35 JPO/Strategic Communication Cell (SCC)/Public Affairs Office (PAO) for a review with a minimum of 15 days prior to the proposed date of release. Lack of response by the FRCSE SSM or the F-35 Program office does NOT constitute approval for public release. Disclosure by the media does NOT constitute approval for public release, additionally anyone who becomes aware of CUI that appears in the media shall report such information to the FRCSE SSM.

(U) The term "information" applies to, but is not limited to articles, speeches, photographs, videos, brochures, advertisements, displays, simulations, and presentations regarding the F-35 program at FRCSE and any connection between FRCSE to any phase or component of the F-35 Lighting II Program.

(U) Prior to submittal to JPO/SCC/PAO, government agencies and defense contractors must review information to ensure it is unclassified, technically accurate and is not considered proprietary. A letter of transmittal must certify this review. Copies of the material may not be released outside official channels until the review process is complete. If information is found during the review process that is suspected of being classified, all holders of the document must be notified as to the degree of protection required. It will be the responsibility of the document's creator to ensure this is accomplished. Information received from contractors for public release will not be considered proprietary. Upon JPO approval, such information will be considered "public domain" and the JPO will have the right to use the data as such.

(U) Resubmit for review and approval any information or materials developed, revised, or modified after initial approval for public release.

3.10 (U) CONSTRUCTION SITE OPERATIONAL HOURS

(U) Work shall be performed during normal duty hours 0700-1600, Monday through Friday. No work shall be performed on Government holidays or weekends. Work may be performed outside of normal working hours, excluding weekends and federal holidays, if approved by the PM and SSM. Changes in the hours of work must be approved by the Government Contracting Agency or PM and the SSM. Changes to work hours shall be submitted by the Prime Contractor to the PM not less than 10 workdays prior to the requested date of effective change. The PM shall notify the SSM without delay of any requested change to work hours.

3.11 (U) SITE SECURITY

(U) The Prime Contractor shall ensure that all measures contained in this CSP, or subsequent approved revisions, are complied with.

3.12 (U) TWO-WAY RADIOS

(U) Two-way radios meeting 47 CFR Part 90—Private Land Mobile Radio Services (§§ 90.1 - 90.1338) may be utilized by the Prime contractor and sub-contractors following written approval by the NAS Jacksonville Frequency Coordinator and the SSM. The Prime Contractor shall submit a request for use of two-way radios to the PM at least 30 work days prior to the introduction of radios to the project site. The two-way radio request shall include the following information:

- Radio manufacturer name
- Radio model name or number

- Specific frequency(ies) transmitted by the radio(s)
- Effective Radiated Power in watts transmitted by the radio(s)
- FCC ID of the radio(s)
- Quantity of radios to be utilized on the project site
- Location the radios will be stored when not in use

(U) All two-way radios shall be procured by the Prime Contractor. No Contractor two-way radio(s) will be permitted within the secure portions of construction area for any reason

3.13 (U) SECURITY INCIDENTS

(U) A security incident is any breach, deliberate or unintentional, of the RFP, to include this CSP, or U.S. Government security policies, regulations, requirements, or procedures. **Immediately report to NAS Jacksonville Police by 911 any Security Incident involving weapons, violence, immediate or imminent threats of harm to persons or to US Government property, or loss or compromise of Classified National Security Information (CNSI).** All security incidents shall be reported immediately to the SSM, or if the SSM is not available the FRCSE Command Duty Officer at 904-891-2782 and NAVFAC PM. Any contractor involved in a security incident shall cooperate fully during the investigation of a security incident. Failure to cooperate in an authorized investigation may result in disciplinary action, including possible removal from the project. The U.S. Government shall not be responsible for security incidents that create an impact to schedule or costs when it is determined, by the appropriate U.S. Government representative that the contractor, sub-contractor, or their employee is at fault or their action were in error.

3.14 (U) SECURITY VIOLATIONS AND REMOVAL FROM THE PROJECT

(U) Any person(s) who violate(s) the requirements of this CSP, willfully ignore(s) or refuse(s) to follow SSM Staff direction or creates an increased risk (intentional or unintentional) to the overall project may be immediately removed from the project by the SSM, up to and including permanent removal from the project. Removal from the project may be temporary or permanent and may include only the secured construction site/SSA or the entire project and all aspects of it, to include removal of access to designs/plans, meetings, and other project activities, Removal from the project shall be a last resort by the SSM exercised only when necessary to protect the integrity of the facility/project and/or the operational and end user mission. Removal from the project for security violation(s) shall be at no cost to the government and to the best ability of the contractor shall minimize delay to the project.

3.15 (U) PHASE OF CONSTRUCTION

(U) For the purpose of this project, the CSP will address the project in three distinct phases: Planning Phase, Construction Phase and Fit-Up.

(U) Planning Phase: The first phase of the project will include the measures leading up to the contract award process including design. The design shall be performed by U.S. companies using U. S. citizens. All information systems shall be approved by the NAVFAC PM and have a current Authority to Operate accreditation issued by the US Government. ***Use of non-U.S. citizens requires prior written approval by the SAO, approval is contingent upon acceptable risk of established mitigations. These mitigations shall be documented in the CSP.*** The NAVFAC PM/CSC shall provide written requests for use of non-U.S. citizens to the SSM a minimum of 21 working days prior to the date of access requested.

(U) Requirements for personnel control of plans and documents and basic information regarding the procurement, transportation, storage, and basic construction security requirements are provided to the construction firm during the planning phase.

(U) Construction Phase: This is the first phase of construction, when the majority of the general construction is completed. This phase will be accomplished with U.S. companies using U.S. citizens, who will be restricted to specified areas of the project, as designated by the SSM. *Use of non-U.S. citizens requires approval by the SAO, approval is contingent upon acceptable risk of established mitigations. These mitigations shall be documented in the CSP.*

(U) Personnel may require escort, or other security protection during this phase of construction. Once all substantial work is completed, Beneficial Occupancy Date (BOD) as defined by NAVFAC will be determined and the appropriate U.S. Government representatives will assume control of the construction site. A final "punch-list" of work to be completed will be created by NAVFAC, with participation from the contractor, SSM, and any applicable elements. Once BOD has been established, the U.S. Government will assume complete control over the work site from the contractor, including lock core or combination changes throughout the facility. At this point only cleared U.S, Citizens with command issued badges will be eligible to work at the site.

(U) Construction Fit-up Phase: The fit-up phase is the second phase of construction will begin upon determination of BOD. Following BOD, the fit-up phase will commence, which will include improvements to, and installations within the facility, requiring work to be completed by U.S. Citizens. Workers without proof of U.S. citizenship will not be permitted access as determined by the SAO or SSM. **Prior to the installation of any type of infrastructure, equipment, etc., interim facility accreditation must be obtained.**

3.16 THREE-WEEK LOOK AHEAD

(U) The Prime Contractor shall provide the SSM and NAVFAC PM a minimum "Look Ahead" of three (3) weeks of the planned schedule and activities on the Project work site. The Three-Weel Look Ahead should be provided using a format approved by the NAVFAC PM.

3.17 (U) LANGUAGE TRANSLATION SERVICES

(U) The Prime Contractor is responsible for providing any and all language translation services for all contracted and sub-contracted employees, at no cost to the U.S. Government.

3.18 (U) EMERGENCY PROCEDURES

(U) FRCSE has existing policies and emergency action procedures in the event of emergencies. Contractor responsibilities for action in the event of emergencies shall be detailed in the indoctrination briefings and documentation provided by designated U.S. Government representatives (e.g. SSM, NAVFAC PM/CSC).

(U) For emergency services the contractor will call 911, or the local emergency number provided during the indoctrination briefing, and specify location of the emergency on Naval Air Station Jacksonville. Initial E-911 calls are routed to Clay or Duval County Public Service Access Points who then transfer the

call to the Commander Navy Region Southeast Dispatch Center. The Navy dispatcher will take the emergency information and dispatch emergency services are required.

(U) The SSM, FRCSE Command Duty Officer at 904-891-2782, and NAVFAC PM/CSC, shall be notified of all emergencies as soon as it is safe to do so. Dissemination of information up the chain of command related to emergencies shall be completed by SSM and FRCSE Command Duty Officer. Information regarding emergencies shall not be released by any party to any person, agency, or organization outside of FRCSE, NAVFAC or COMFRC without written permission from the FRCSE or NAVFAC Public Affairs Office.

The SSM will be responsible for all security decisions during an emergency/accident and at all times life safety considerations shall take precedence over security.

3.19 EMERGENCY SERVICES ACCESS
(U) NOTE : During a bomb threat, no radios or wireless communications devices shall be used.

(U) In the event of an emergency / accident that requires outside/off site assistance, e.g. fire, paramedics, or law enforcements; the personnel on the project site shall notify the of the need for emergency services via telephone to 911, or by the most expeditious way possible, if a telephone is not available.

(U) In the event of fire all efforts shall be made to raise the alarm to all personnel in the area, and the building fire alarm shall be activated if possible. The FRCSE CDO and SSM shall be notified without delay. The SSM shall notify the NAVFAC PM and the Prime Contractor Foreman. Emergency response personnel will be allowed immediate and unimpeded access to the emergency location. Immediate and unimpeded access shall not be granted to non-emergency personnel.

(U) The SSM Staff shall monitor an emergency personnel when on the SCS/SSA as closely as possible, without interfering with emergency personnel operations and always from a safe distance. Emergency personnel shall be subject to search, with coordination of the Incident Commander, when exiting the SCS/SSA as long as the emergency has been adequately addressed and no longer deemed an emergency. If emergency personnel need to leave the site as part of their emergency operations, e.g., an ambulance leaving with an injured person; they will be allowed immediate and unimpeded access from the project site.

3.20 (U) SAFETY
The GC is responsible for the safety of this project site, not the SSM nor SSM Staff. SSM Staff members shall not interfere with the job duties/responsibilities of the safety officers on the project site unless it directly relates to the security of this project. Safety officers shall not interfere with the operations of the SSM Staff unless it is a life safety issue. Non-life safety issues related to the SSM Staff shall be brought directly to the SSM and/or NAVFAC PM. The SSM shall ensure that all SSM Staff members perform their job duties and responsibilities in a safe manner and in accordance with US and local laws and DoD/DoN policy and regulations.

3.21 (U) WORK STOPPAGE

(U) in the event of an exceptional security incident, or perceived incident, that could potentially affect the integrity of the building or facility, compromise the end user mission, impact final accreditation, or anything else deemed necessary by the SSM, the following steps will be followed in order until the situation is resolved:
1) The SSM staff member will notify the SSM mediately, who will contact the Sao immediately.
2) If deemed necessary, the SSM has the authority to initiate a work stoppage and have all personnel vacate the job site, or the area of concern. This will allow authorized personnel to conduct a security investigation.
3) The SSM staff will secure the job site perimeter until authorities arrive.
4) The investigation will terminate, and work will resume only at the discretion of the SAO and SSM

(U) If the security incident, or perceived incident, is determined to be caused by a Prime Contractor, or sub-contractor employee, other than the security contractor, the US government shall not be responsible or at fault for any lost time, production, or construction delay.

4.0 PLANNING PHASE

4.1 (U) VISITORS

(U) Visitors are identified as any person who does not require daily or routine (more than three (3) times per week) access to the Project site. Visitors will be categorized as “Infrequent visitor approved for project site access” “Unvetted Visitor” or “Emergency Access”.

(U) Infrequent visitors approved for site access will comply with sections 3.5.1 or 3.5.2 of this CSP prior to being granted unescorted access to the Project Site.

(U) Unvetted visitors’ are anyone who does not meet compliance with sections 3.5.1,.3.5.2. Unvetted visitors shall be permitted escorted access to the Project site only in exceptional circumstances with the direct approval of the SSM.

(U) Emergency Access visitors’ are credentialed Emergency Responders in the performance of their duties and responding to a bona fide Emergency on or immediately adjacent to the Project work site. Emergency Access visitors shall to the best ability of the SSM, be escorted by Cleared U.S. Government Civil Service emploees cleared for access to the Project site

(U) All persons shall be vetted by the SSM prior to being authorized access to the project areas except for credentialed emergency responders actually responding to an emergency in the area of the project. Emergency responders include fire department, law enforcement, emergency medical and NAS Jacksonville or FRCSE civil service employees directly supporting the emergency response. The emergency response period shall be considered as over when fire department, law enforcement or emergency medical services have cleared the project area. All project area access vetting shall be accomplished in accordance with the current FRCSEINST 5500.5 and FRCSEINST 5510.14 instructions.

4.2 (U) ESCORTS

(U) Escorts are U.S. Government personnel with special U.S. Government clearances responsible for securing the construction site. Escorts shall be used during the project as directed and in accordance with the current issued revision of the FRCSEINST 5500.5 Physical Security Plan. Specific areas and escort numbers will be determined based on the requirements of each aspect of the project. Escorts will be provided training by the Security office on escorting duties and inspection procedures for prohibited items. When specifically employed, contracted Construction Surveillance Technicians may also be used for escorting and inspection duties.

4.3 (U) CONSTRUCTION SECURITY TECHNICIAN

(U) See Appendix H

4.4 (U) ACCESS CONTROL

(U) There will be a designated Entry Control Point (ECP) at the construction site for personnel and vehicles, which shall be managed by government representatives at the construction site, at all times. Generic, laminated badges will be used to control and identify vetted contractors for entry into the facility and construction site. The SSM will maintain an access log to document all personnel granted access to the Fixed Facility. Access log will include, at a minimum; full name, organization, date, entry time, exit time, and purpose for access.

(U) The NAVFAC PM/CSC shall compile a list of all contractor vehicles requiring regular access to the construction site for more than 30 days. Vehicle access is limited to U.S. government or contractor company owned/leased vehicles. Personally owned vehicles are prohibited from accessing the FRCSE Level Two Restricted Area. Deliveries/drivers to the construction site will be escorted by a designated government escort. Personally owned vehicles of contractors are required to be parked in specified areas outside the construction site, as not to interfere with access and work on the site. Personnel bringing approved vehicles onto the construction site must possess a valid construction site badge. Vehicles requiring access to the construction site will require a site-specific vehicle pass and are subject to inspection by the SSM and/or designated security representative.

4.5 (U) BRIEFING REQUIREMENT

(U) Upon completion of vetting, all assigned personnel will receive appropriate security briefings from the SSM related to the protection of the construction site. All applicable security policies will be briefed to the contractor prior to access being granted. Contractor personnel must abide by all regulations and procedures established by the SSM. Failure to comply with any of these policies, regulations, or procedures may result in the offending person being removed from the site and/or project.

(U) Completion of briefing by the SSM is a requirement for issuance of a construction site identification badge. All personnel used in the third phase, referred to as “Fit-Up”, will be required to attend an additional security briefing tailored to this construction phase, which will differ from the initial construction phase. This briefing will last approximately one hour, and documents related to this briefing will be supplied by the SSM. A Non-disclosure Agreement Standard Form 312 (SF 312) will be completed by all persons involved in the “Fit-Up” if a record is not available of a SF 312 having been completed in the last 10 years. Additional Non-disclosure Agreements or Non-disclosure Statements may be required during this project, as determined by the SAO or SSM.

4.6 (U) BADGING REQUIREMENT

(U) All FRCSE 5500/17 FRCSE Visit Access Badge Request will be submitted to the SSM for review, vetting, and approval. A badge for access to the FRCSE work site will be provided by the command once U.S. citizenship has been verified, favorable SAO vetting approval is received, and the required briefs completed.

(U) The current issued revisions of the FRCSEINST 5500.5 Physical Security Plan and FRCSEINST 5510.14 Information, Personnel, and Industrial Security Procedures will dictate the background investigation, U.S. Citizenship verification, and badging issuances. The FRCSE 5500/17 FRCSE Visit Access Badge Request will be used for all badging issuances. Two sponsors are required for approval of FRCSE badging. Sponsors include NAVFAC PM/CSC, Contracting Officer (KO), Contracting Officer Representative (COR), Assistant Contracting Officer Representative (ACOR), Task Order Contracting Officer Representative (TOCOR), or substantially similar U.S. Government officials. Badging requests must be submitted to the SSM at least five (5) working days prior to date requested for access.

(U) Issued badges must be prominently displayed at least 6 inches above the waist and below the shoulders, outside of all layers of clothing for ease of identification at all times while on the construction site. The badges are the property of the U.S. Government and will be created and issued at the project site location. A badge clip will be provided for the display of the site badge. The SSM will designate a government security representative to supply and manage the issuance of site generic construction badges. All temporary access badges (day badge) will be returned to issuing point at the end of each workday prior to worker departure and accounted for by the government security representative. Lost or stolen badges shall be reported to the site government security representative and SSM immediately. When an individual no longer requires access, or is removed from access, the badge shall immediately be returned to the SSM or designee.

(U) The SSM shall create an access roster after SAO vetting. The roster shall be returned to the designated U.S. Government security representative. At this point, badges from the construction phase will no longer be accepted for access to the site. During Fit-up, cleared government personnel with command issued badges will be authorized entry based on the access roster provided by FRCSE Security.

4.7 (U) PROHIBITED ITEMS

(U) There are certain items that are prohibited from introduction to the construction site. Only the SSM has authority to grant waivers for these items as deemed necessary for the performance of this contract. The Prime Contractor shall provide weatherproof signs with font not less than 16 point, in English, to the SSM for posting at all project site entry points that identify prohibited items. Signs shall be provided to the SSM not less than 10 workdays prior to the first contractor arriving for work. A digital example or physical sample of prohibited item signs shall be provided to the SSM and NAVFAC PM not less than 20 work days prior to the first contract worker arriving at the project site.

Any requests for prohibited item exception shall be sent to the SSM in writing from the Prime Contractor no less than five (5) business days prior to attempting to bring the item onto the project site. The Prime Contractor is responsible for notifying their personnel and all subcontractors about these restrictions prior

to accessing the project site. The Prime Contractor is responsible for providing a storage location for cell phones, key fobs, and any other devices that their employees cannot bring onto the project site.

(U) The following list of prohibited items apply, will be included as part of the security briefing, and will be posted at the entry control point:

- Firearms, weapons, and ammunition. Exceptions will be made for tool items, such as multi-tools with small blades not exceeding 3½ inches. Tools requiring the use of powder charge cartridge or other explosive charges must be submitted to the NAVFAC CSC who will forward the information to the NAVFAC PM and SSM for approval. Powder charge operated devices and powder charge cartages will be transported, stored, and used in accordance with the directives of the NAVFAC PM/CSC and the NAS Jacksonville Explosives Safety Officer. Questions or concerns related to powder charge operated devices and powder charge cartages will be directed to the NAVFAC PM/CSC and the NAS Jacksonville Explosives Safety Officer.
- Explosives or incendiary devices, except as noted for powder charge operated devices above.
- Cameras, photographic equipment, or other equipment capable of recording audio/video/images. Cell phones will not be permitted on the construction site without written permission issued by the SSM. Persons found using cameras or other recording devices are subject to having those devices confiscated for review and for potential destruction. On-site photography will only be conducted with written SSM approval, with a government-owned camera, with all images subject to review and government approval for release. A copy of the written approval shall be maintained with the camera or recording device while on the project site.
- Personally owned or contractor-owned, electronic devices capable of information storage (media storage devices), i.e. cell phones, flash drives, tablets, smartwatches, and other devices that can record or transmit data, test measurement or diagnostic equipment, digital music players, and read/write optical disks are restricted from introduction into operational areas and other sensitive areas designated by the SSM. Exceptions to the above will require written approval by the SSM and/or SAO.
- Sound or video recording equipment, devices capable of capturing audio, or visual imagery, or Light Detection and Ranging (LiDAR) devices, except as approved in writing by the SSM for work related activity.
- Illegal, alcoholic and/or intoxicating beverages, food or substances, non-prescription drugs. Prescription medication shall be maintained in the pharmacy or physician issued container with a legible label.
- Two-way radios, except as approved by the SSM for work related activity.
- Drone or remotely operated unmanned arial or ground vehicles without written authorization.
- Construction tools containing two-way communications such as cellular, wireless fidelity wireless network protocols (Wi-Fi), BlueTooth, nearfield communications (NFC), or other RF communications devices unless expressly approved in writing by the SSM.
- Exceptions may be requested in writing from the Prime Contractor for devices by submitting such request to the SSM, via the NAVFAC Project Manager, not less than 30 days prior to the planned use of the device or tool. The use of the device shall not be permitted unless written approval from the Accreditation Official is received. A copy of a written approval shall be maintained with the SSM and the tool or operator at all times while the tool is used on the project.

(U) The Accreditation Official, through the SSM, maintains approval or disapproval authority of prohibited items, based on risk determination. The NAVFAC PM is responsible for providing information to the contractors regarding NAS Jacksonville and FRCSE regulations. Prohibited and Restricted Items lists are subject to review and change, with additional items added subsequently. The SSM will advise the NAVFAC PM of any changes made to the prohibited/restricted items lists. The NAVFAC PM is responsible to advise contractor of any changes made to the prohibited/restricted items lists.

4.8 (U) INSPECTIONS

(U) All personnel, vehicles, materials, storage or transportation containers, and equipment entering NAS Jacksonville and the construction site are subject to search and inspection by designated U.S. Government personnel. Naval Air Station Jacksonville maintains independent inspections for access to the base; details regarding entry will be supplied by NAVFAC. Individuals found in possession of prohibited items may be required to remove them from site and/or could be subject to disciplinary, legal, or law enforcement action based on the nature of the item. Possession of items in violation of local, installation, state, or federal law may necessitate the involvement of local law enforcement authorities and Navy Criminal Investigative Service.

(U) The SSM or government-designated security representative will inspect materials for tampering and suitability and will reject items that show signs of tampering or that are not suitable for construction.

(U) The SSM or designee will use metal detection devices for screening all persons entering the secure portions of the construction site as identified by the SAO or SSM for prohibited items as identified elsewhere in the Construction Security Plan.

(U) Materials used for construction of the Secure Area will be stored inside a locked container within the controlled construction area as designated by the SSM. In the event of loss of positive U.S. control of the storage container or materials, the Contractor will notify the NAVFAC PM/CSC, and the Contracting Official Representative (COR) without delay, but not later than 2-hours after discovery of suspected loss, tampering, or compromise. The NAVFAC PM/CSC will provide notification to the SSM within one (1) hour. The SSM will provide voice notification to the FRCSE CDO and SAO without delay and provide amplifying information as it becomes available. If theft or tampering of materials is suspected the SSM will notify NAS Jacksonville Police for investigation.

(U) The contractor's schedule will identify milestones that require SSM or government designated security representative inspection before the contractor is allowed to proceed. Milestones include inspection of new construction materials, and/or activities such as permanently sealing areas or points from access or inspection, inspection of construction. The SSM or government designated security representative will document inspection of such milestones in the daily logs.

4.9 (U) PERSONNEL ACCESS ENTRY CONTROL POINT (ECP) AT CONSTRUCTION SITE:

(U) There will be a designated ECP for personnel and vehicles at the construction site. All personnel, equipment, and/or vehicles requiring access to the controlled construction area must enter through the ECP. A cleared U.S. Government representative will be onsite and within the controlled construction

area at all times when the worksite has ongoing operations for the purpose of issuing access control badges, controlling access to the site, and inspecting for prohibited items. A list of prohibited items shall be posted at the ECP.

(CUI//NF) The controlled construction area beyond the ECP shall be verified to be cleared of all persons and the ECP gate locked whenever there are no construction or associated activities ongoing. Prior to locking the ECP Gate a cleared person will conduct a sweep of the entire controlled construction area to verify no one is within the area. During the area sweep a cleared U.S. Government representative will be posted at the ECP to ensure no one enters the controlled construction area. Upon the conclusion of the controlled construction area the U.S. government representatives will close and lock the ECP gate, attach a numbered seal, and compete the SF 701 and SF 702 at the ECP, with the person performing the sweep completing the Checked By portion of the SF 702 certifying the controlled construction area is cleared of all persons and the ECP gate is locked.

(U) Only personnel on the access roster will be issued badges and granted access within the controlled construction area. Government-issued generic badges will be used to identify vetted contractors and/or civilian personnel for entry into the Fixed Facility controlled construction area.

(U) All personnel, vehicles, materials, and equipment entering the construction site is subject to search and inspection by designated US Government personnel. Naval Air Station Jacksonville maintains independent inspections for access to the base; details regarding base entry will be supplied by NAVFAC. Individuals found in possession of prohibited items may be required to remove them from site and/or could be subject to disciplinary or legal action based on the nature of the item. Possession of items in violation of local or federal law will necessitate the involvement of local law enforcement authorities.

(U) Visitor Access: Notification of visitors must be made in writing at least five (5) working days prior to the date of the visit to the NAVFAC PM/CSS and SSM in advance of any visitor requesting access to the Fixed Facility who is not on the access roster. Visitor clearance information for all visitors shall be submitted to the SSM using the Defense Information System for Security (DISS) using Security Management Office (SMO) code N658865. An official Visitor Request by the contractor and/or government entity shall be submitted by email to the SSM by NAVFAC. Visit notification email shall include the beginning and end dates, SMO of the submitting DISS account, and name of the visit as indicated in DISS. If DISS cannot be used for notification, the visit and visitor information will be submitted the SSM in writing. The written visit request will include the identification of all visitors to include the following:

- Agency/Company name and address
- Date(s) of visit
- Purpose of visit
- Contract number (if applicable)
- Visitor's full name, social security number, date of birth, and place of birth
- Citizenship/Nationality (if Naturalized Citizen, provide Certificate of Naturalization Number)
- Date Form I-9 and/or E-Verify processed (if applicable)
- Clearance data (clearance eligibility/level, agency who granted clearance and date granted)

- Level of Access Required
- Agency/Company clearance data (clearance and safeguarding levels, date granted and CAGE code, if applicable)
- Agency/Company Security Officer's full name, telephone number, email address
- Government Sponsor (e.g. COR) full name, telephone number, email address

4.10 (U) PROCUREMENT OF NON INSPECTABLE MATERIAL

(U) All procurements shall be in accordance with Federal Acquisition Regulations. The prime contractor will be responsible for procuring all construction material for the construction of this facility including Fixed Facility related construction.

(U) The prime contractor will identify all subcontractor and vendor candidates to NAVFAC and the SSM at least 45 days before their services are required for screening. OPSEC, random selection, inspection and secure storage are the prime risk mitigation strategies that will be used for Fixed Facility construction materials.

(U) For this Construction project, the U.S. Government may randomly select up to 35 percent of building materials from non-specific general construction materials. Ultimate use of the materials will not be disclosed to the vender. Non-inspectable materials will be procured from U.S. suppliers. Materials shall be randomly chosen from available suppliers (preferable three or more) without advance notice to or referral from the selected supplier and without reference of the intended use of material in a fixed facility / secure area. Selections shall be made from an available shelf stock and transported securely to a Secure Storage Area (SSA).

4.11 (U) STORAGE OF CONSTRUCTION MATERIAL

(U) Contractor shall establish a Secure Storage Area (SAA) for the secure storage of all fixed facility / secure area construction material and equipment. The SSA will be true floor to ceiling and slab construction of some substantial material and a solid wood core or steel-clad door equipped with a high security lock. The SAA will be under the control of the SSM or a U.S. person possessing at least a U.S. Secret clearance. Electrical and mechanical materials will be relocated inside and secured at the end of the workday by the SSM and/or designated government security representative. Materials brought to the site shall not be removed from the site, except with the permission from NAVFAC and the SSM.

4.12 (U) CONSTRUCTION SECURITY REQUIREMENTS CONTROL OF PLANS AND DOCUMENTS

(U) All plans and documents, including electronic and hard copy, shall be controlled in accordance with this Security Plan, and as follows:

- All plans and documents, including electronic and hard copy, shall be controlled as Controlled Unclassified Information at a minimum. "CUI" shall be printed on the top and bottom of all paper documentation. The Controlled Unclassified Information shall also be properly marked including the CUI control marking, CUI category markings, and Limited Dissemination Control Markings.
- All CUI documents shall be covered with the CUI cover Sheet, Standard Form 901 (SF 901). Removable electronic media such as Compact Disks (CD, Digital Video Disks (DVD), USB hard

drive, solid state drive, and flash drive devices shall be labeled with appropriate CUI markings including SF 902 CUI or SF 903 labels.

- Project documents provided by the U.S. Government may not be reproduced by the sub-contractor, either whole or in part, without approval from the U.S. Government. All documentation provided by the U.S. Government is Controlled Unclassified Information (CUI) and is accountable. These documents are not releasable without the approval of the U.S. Government.
- Commercial cloud computing services used in the processing, storage, or transfer of project documents shall comply with the DoD Cloud Computing Security Requirements Guide (SRG) and the DFARS clause 252.239.7010, "Cloud Computing Services". Cloud computing services used for unclassified and controlled unclassified information shall meet the security requirements of Impact Level 5 (IL5) at a minimum. Commercial cloud computing services used in the processing, storage, or transfer of for classified project documents and/or information up the to the level of GENSER SECRET shall meet the security requirements of Impact Level 6 (IL6) at a minimum. Commercial cloud computing services shall not be used for any classified information above the level of GENSER SECRET.
- Contracting companies shall maintain sufficient records to detail accountability for all copies of provided documents. At a minimum, the records must contain the names of all persons issued documents along with a detailed description of the documents provided.
- Personnel shall verify documents are returned to their control when no longer needed by personnel within their organization.
- When not in use, U.S. Government personnel, prime contractor, and sub-constructors shall ensure that documents are stored in a manner that does not readily provide access of the documents by unauthorized personnel. Acceptable storage included in a locked cabinet or file container within a room controlled by the contractor or U.S. Government that is locked when not occupied.
- When CUI documents are no longer required for project use or records keeping, or have been spoiled or damaged beyond use, they shall be destroyed or returned to the SSM for destruction as specified in the sub-section below.
- Electronic transmission of CUI information (e.g. data, website, or email) shall be encrypted by approved secure communications systems or systems utilizing Public Key Infrastructure (PKI). protective measures. This includes all company generated documentation that is identified for a secure area, to include plans, diagrams, etc. If such measures are not available, the use of the U.S. government Department of Defense (DoD) Secure Access File Exchange (SAFE). Per Office of the Secretary of Defense (OSD) guidance, DoD SAFE should NOT be used for transmission of contract proposals or other contract award documentation. Instead, OSD directs that the Procurement Integrated Enterprise Environment (PIEE) be used for time-sensitive contract submissions and related documentation.

(U) A projects tracking system may be used through an Internet connection that adheres to the following guidance:

- The system shall utilize an https site or commercial encryption and all users shall be required to login with a unique username and password.
- Access shall be restricted to employees, personnel from the U.S. Government and subordinate contractors that have a proven need to access project information and documentations.

- The server for any such processing, storage, and/or access of material will be secured in a lockable building, areas, room, or container belonging to the Prime Contractor.
- Prime contractors who do not have internal project tracking system that meets the above noted requirements may contract for this service with an authorized sub-contractor, with the approval of the government designated COR. The sub-contractor providing this service shall comply with the project tracking system requirements set forth in this paragraph.

(U) The following language will be included on the cover pages of the information, hard copy material, electronic, and/or on the label of all magnetic media:

"Only persons that have been vetted and approved for access to Project program material shall be allowed access to these documents, which are Controlled Unclassified Information. Reproduction of material is not authorized without prior approval by government representative."

"All drawings, plans and designs are the property of the United States Government. Copying, Dissemination, or Distribution of these drawings or Specifications to any unauthorized person is prohibited."

(U) At the conclusion of the project, or when no longer required, the contractor shall return all project documents, along with records used to detail accountabilities for all copies of provided documents to authorized employees, and to the U.S. Government. The NAVFAC CSC and SSM will conduct an inventory of returned project documents against record logs to ensure all project documents have been returned. Discrepancies identified will be addressed with the prime contractor for document control resolution. The SSM will be responsible for ensuring all project documentation retuned by contract are destroyed in accordance with U.S. Government policy. The return location shall be on the project site, as specifically designated by the SSM. Digital copies of documentation shall be permanently deleted when no longer needed.

(U) All drawings, specifications, and documentation, including any copies made or provided to the sub-contractors are the property of the U.S. Government and shall be returned as part of the contract closeout. A letter certifying the return of these materials shall be forwarded to NAVFAC within 30 days of contract closeout.

(U) All sub-contractors must also comply with the above noted document control policies.

4.13 (U) PHOTOGRAPHY OF CONSTRUCTION

(U) The SSM or designee (i.e. Construction Security Technician) will be responsible for taking photographs as the Secure Fixed Facility is being constructed. Pictures will be taken of the walls, ceiling, doors, HVAC/utility penetrations, cable installs, and any other actions in the facility. The purpose of the photos is to record the process of the construction. (e.g. Photos will be taken when the wall studs are installed, when one layer of dry wall is installed on the studs, when the sound batting is installed, when the next layer of dry wall is installed, and then when the final layer of dry wall is installed).

(U) A government owned project-dedicated camera, will be used to photograph each construction phase of the Secure Fixed Facility, as noted above. The camera will be under the physical control of the SSM or designated government security representative, at all times. The SSM will be responsible for reviewing and downloading of pictures for permanent retention at the end of each day, as applicable. Government personnel authorized to take photographs will bear a FRCSE-issued Photography Site Specific Pass, to be attached to the camera, in addition to the site access badge. No pictures will be taken by any of the contractors for company specific marketing. All photos must be approved by the SAO for release outside the accreditation package requirements. All photos will be appropriately marked and controlled in accordance with the DoDM 5200.01 Volumes 1 through 3 and the DOD Instruction 5200.48 Controlled Unclassified Information (CUI).

4.14 (U) PENETRATIONS

(U) The contractor shall build an example mock-up wall depicting examples of the correct construction of all wall penetrations. The mock-up wall shall be placed in a location near the secure facility construction location for use by construction workers as a reference for construction. The example mock-up wall shall be completed and in place prior to the construction of any boundary wall penetrations.

(U) Utilities shall enter the secure area at a single point.

(U) Utilities servicing areas other than the secure area shall not transit the secure area unless mitigated with SAO approval. All penetrations of perimeter walls shall be kept to a minimum.

(U) Acoustic sealant shall be used around all secure area perimeter walls and penetrations.

(U) Sound baffles will be installed in all penetrations of interior boundaries as indicated on construction documents.

4.15 (U) VENTS AND DUCTS

(U) HVAC penetrations shall be documented as 'CALL OUT's' on official blueprints and be kept less than 96 square inches where feasible. Penetrations greater than $0.062m^2(86in^2)$ will have man bars installed with access panels located on the secure side of the HVAC ducting to view the man bars both internally and externally to the HVAC ducting. ***All ducts/vents that are greater than 96 square inches will be documented as 'CALL OUT's' specifically identifying them as large penetrations on official blueprints and forwarded for review***. Man-bars and sound baffles will be installed in accordance with IC Tech Spec-for ICD/ICS 705.

4.16 (U) SOUND ATTENUATION AND ACOUSTICAL SECURITY

(U) Perimeter walls and doors shall meet minimum acoustic security standards as rated by the Apparent Sound Transmission Class (ASTC) value at the time of acceptance by the US Government. These values must be designed and constructed to meet ASTM International (ASTM) (formerly American Society for Testing and Materials) E336 standards of ASTC 55 or better. All areas within the secure facility must be designed and constructed to meet ASTM-E336 standards of ASTC 55 or better. All sound attenuation shall be field tested following construction of the Fixed Facility using calibrated electronic measurements based upon the ASTM-E336 standard. Sound attenuation testing shall be performed by a third party with

documented past performance in performing instrumented sound attenuation testing and agreed to by the SAO, SSM and Project Manager. All instrumented testing that is conducted must be compliant with ASTM-E336 dictates and certified results documenting ASTC results shall be provided to the NAVFAC PM and SSM for acceptance within 5 working days of the completion of the testing.

(U) Any failed sound attenuation shall be corrected by the contractor to correct any deficiencies at no cost to the Government. A passing test result shall be provided to the SSM and NAVFAC PM prior to acceptance of the Project by the U.S. Government.

4.21 (U) DI-ELECTRIC BREAK

(U) All penetrations (vents, doorways, conduit, cable entrances/exits, etc.) at the enclosure shall provide a minimum of 80 dB of Radio Frequency shielding and filtering. For example, honeycomb filters used for air vents or beryllium copper finger stock used with a shielded door to ensure positive contact of the door to the enclosure door threshold.

4.22 (U) FILTERS AND GROUNDING

(U) Filters shall provide a minimum of 60 dB of insertion loss when tested IAW Military Standard (MIS-STD)-220C and shall be installed on all wire lines that penetrate the shielding. Test frequencies shall be within the test frequency ranges of IEEE Standard 299-2006 as stated in paragraph 6.1.2.

(U) Power filters and signal filters shall be grounded to the shielded area. Ground Plane Requirements: An equipotential ground plane shall be used for signal grounds IAW Federal Information Processing Standards Publication (FIPS PUB) 94 and/or MIL-HDBK-419, Volume II. The shielded area shall be tied into equipotential ground plane.

(U) Any failed tests shall be corrected by the contractor to correct any deficiencies at no cost to the Government. A passing test result shall be provided to the SSM and NAVFAC PM prior to acceptance of the Project by the U.S. Government.

4.23 (U) CRITICAL INFRASTRUCTURE

4.24 (U) CONSTRUCTION SECURITY TECHNICIANS (CST)

(U) Construction security technicians will be contracted through a third party security contractor for the duration of this project from 14 calendar days prior to commencement of any phase of construction until 14 days following completion of construction, Fit-up, finish work, and final completion of furniture, fixtures, and equipment and acceptance of the secure fixed facility by the government.

(U) The Prime Contractor shall coordinate with the SSM using the three-week look ahead for all work requiring CTS monitoring to ensure adequate CST staff is available to monitor this work. The Prime contractor and the NAVFAC PM shall ensure that all reasonable efforts are made to schedule and phase work in such a fashion that CST's are reasonably expected to be available for the monitoring of such work. The SSM and U.S. Government shall not be responsible for work delays caused by unreasonable or short notice, i.e. not so indicated on the three-week look ahead workload, CST requirement

expectations proposed or scheduled by the Prime Contractor or sub-contractors that result in the non-availability of the construction security technicians assigned for this project.

5.0 CONSTRUCTION PHASE

5.1 SECURE CONSTRUCTION SITE FENCE

(U) The Prime contractor shall install an 8-foot high chain link fence barrier with a single swing gate around the secure fixed facility construction footprint at a distance not less than 10-feet not more than 15-feet from the outer edge of the West, North and East sides of the secure fixed facility footprint. The fence shall be securely fixed and physically connected to the floor and existing south wall of the space designated for the secure fixed facility. The swing gate shall be located on the West side section of the fence. The fence and swing gate shall be designed and installed using the reference information contained in the United Facilities Criteria (UFC) 4-022-02 Security Fences and Gates and designs contained in the associated UFC-700 and UFC-702 Drawing Details.

(U) The security fence may be removed following the activation and acceptance of the secure fixed facility ESS. Request to remove the security perimeter fence shall be submitted to the SSM in writing by the prime contractor at least 5 days prior to the date of requested removal.

5.2 ROUGH-IN FOR MECHANICAL, ELECTRICAL, PLUMBING, AND COMMUNICATIONS

(U) All rough-in for mechanical, electrical, plumbing, and communications installation shall be under direct CST supervision. The prime contractor shall clearly identify on the three-week look ahead all rough-in for mechanical, electrical, plumbing, and communications work. Exceptional cases for emergent or urgent rough-in work shall be communicated to the SSM at least 72 hours in advance. If the prime contractor does not notify the SSM at least 72 hours in advance of rough-in work, the SSM may deny the rough-in work at no cost to the government due to failure for the prime contractor to meet the requirements of the CSP

5.3 CLOSE-IN AND SEAL-IN REQUIREMENTS

(U) All close-in and seal-in work shall be under direct CST supervision. The prime contractor shall clearly identify on the three-week look ahead for all close-in and seal-in work. The prime contractor shall include all close-in/seal-in activities on the three-week look ahead schedule. Exceptional cases for emergent or urgent close-in/seal-in work shall be communicated to the SSM at least 72 hours in advance. If the prime contractor does not notify the SSM at least 72 hours in advance of close-in/seal-in work, the SSM may deny the close-in/seal-in work at no cost to the government due to failure for the prime contractor to meet the requirements of the CSP

(U) Close-in and seal-in work is considered to be “Any point in the construction or any work activity that upon completion will result in an area being closed or sealed off from post work inspection by the CST staff”.

5.4 LOGICAL PROGRAMMING

(U) All materials and equipment that require programming shall be programmed under direct construction security technician supervision. The prime contractor shall clearly identify on the three-week look ahead all logical programming work. Exceptional cases for emergent or urgent logical programming work shall be communicated to the SSM at least 72 hours in advance. If the prime contractor does not notify the SSM at least 72 hours in advance of logical programming work, the SSM may deny the logical programming work at no cost to the government due to failure for the prime contractor to meet the requirements of the CSP

(U) Computers required for this programming shall be requested to be brought into the secure fixed facility to the SSM no less than 21 calendar days prior to their intended use. The SSM may require the computers be delivered to the SSM prior to their use for inspection by the US government. The prime contractor and /or subcontractor shall provide the computer, software, and all components required for operation (EG power cord, computer password, software password, etc.) Requests for exceptions to this requirement shall be made to the SM in writing and a final determination will be made after the Sao and SSM collaboration. Materials, components, parts, etc for any system shall not be delivered to these secure fixed facility or secure storage area already programmed for use, nor labeled for a specific room or room number where they are intended to be installed. Examples of systems that cannot arrive preprogrammed include but are not limited to:

- Building automation system or building management system
- Fire alarm system or mass notification system components or sensors
- Thermostats
- Computer room air conditioner units
- Air handling units
- Variable air volume controllers
- Uninterruptible power supply systems

5.5 (U) KEY CONTROL

(U) Critical keys to the construction site and SAA shall be strictly controlled by the SSM, or designated U.S. Government appointees. Keys will be inventoried and properly secured at the end of each day. All construction keys are to be serialized; duplication of all critical key requires written approval from the SSM. At no time will keys to any doors, gates, etc. be given to any contractor personnel for any reason. If the contractor personnel require access to an area that is locked, the SSM or designated government security representative will obtain the keys and grant access in accordance with site procedures.

(U) Unauthorized possession of keys, loss, theft, or any other issue that leaves keys unaccounted for shall be immediately reported to the SAO by the SSM for risk determination. The SAO will make the final determination related to mitigations and/or rekeying of locks.

5.6 (U) TOOL STORAGE

(U) All tools and toolboxes, tool bags, and tool containers are subject to inspection upon entry to the construction site. Additional inspection of all tools and related items may be required upon entry to the Secure Fixed Facility construction area. Workers should be encouraged to store tools on site, especially tools used for the Secure Fixed Facility, to eliminate the need to reintroduce and inspect these items daily. The contractor(s) are responsible for the securing/protection of the tools left on site. The U.S.

Government will not be responsible for lost or stolen tools on the work site. Spaces designated for tool storage can be inspected by U.S. Government personnel for prohibited items, at any time.

5.7 (U) FIT-UP / FINISH WORK

(U) All Fit-Up and Finish work shall be performed by U.S. Citizens holding an active Eligibility Level of Top Secret or higher with Access to at least the Top Secret level as indicated in DISS. A DISS Visit Request shall be submitted to SMO N658865 for all personnel requiring access to the secure fixed facility during Fit-Up and Finish work. Each Contractor FSO shall submit a single DISS VR for all

(U) **IDS/CRITICAL INFRASTRUCTURE/IT COMMUNICATION EQUIPMENT**
(U) All personnel used in the second phase, referred to as "Fit-Up" will be required to attend a security briefing tailored to this construction phase, which will differ from the initial security briefing.

5.8 FURNITURE, FIXTURES, AND NON-IT/ADP EQUIPMENT
(U) All furniture, fixtures and non-IT/ADP equipment installation shall be under direct CST supervision. The prime contractor shall clearly identify on the three-week look ahead all furniture, fixtures, and non-IT/ADP equipment installation work.

5.9 IT/ADP EQUIPMENT INSTALL
(U) All IT/ADP equipment installation shall be under direct CST supervision. The prime contractor shall clearly identify on the three-week look ahead all IT/ADP equipment installation work. Any IT/ADP equipment installed outside of the Prime Contractor responsibilities shall be coordinated with the SSM at least 30 calendar days prior to installation great

5.10 SOUND CONTROL TESTING / INSPECTION
(U) All sound attenuation shall be field tested following construction of the Fixed Facility using calibrated electronic measurements based upon the ASTM-E336 standard. Sound attenuation testing shall be performed by a third party with documented past performance in performing instrumented sound attenuation testing and agreed to by the SAO, SSM and Project Manager. All instrumented testing that is conducted must be compliant with ASTM-E336 dictates and certified results documenting ASTC results shall be provided to the NAVFAC PM and SSM for acceptance within 5 working days of the completion of the testing.

Any failed sound attenuation shall be corrected by the contractor to correct any deficiencies at no cost to the Government. A passing test result shall be provided to the SSM and NAVFAC PM prior to acceptance of the Project by the U.S. Government.

5.11 HVAC TESTING AND BALANCING
(U) All HVAC testing and balancing shall be under direct CST supervision. The prime contractor shall clearly identify on the three-week look ahead all HVAC testing and balancing work.

5.12 IEEE 299 RF TESTING / INSPECTION
(U) Perimeter walls and doors shall meet the criteria specified by the project Design Specifications for RF shielding (TEMPEST) prior to acceptance of the finished project site by the US Government. TEMPEST testing shall be performed by a company listed on the National Security Agency TEMPEST Certification

Program listing provided by the SSM, or a company with documented past performance in performing instrumented TEMPEST testing and that is approved in writing by the SAO. All instrumented testing that is conducted shall be in accordance with the NSTISSAM TEMPEST/1-92 and CNSSAM TEMPEST 01-02, and IEEE 299 RF Testing specifications. Certified TEMPEST testing documentation results shall be provided to the NAVFAC PM and SSM for acceptance within 5 working days of the completion of the testing.

5.13 PUNCHOUT/ACCEPTANCE CHECKLIST

ANNEX A: NON-DISCLOSURE AGREEMENT

U.S. Navy, Fleet Readiness Center Southeast Construction Project
NAS Jacksonville, Jacksonville, FL

Controlled Unclassified Information Non-Disclosure Agreement

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ , (the Authorized Entity), intending to be legally bound, hereby consent to the terms this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

As used this Agreement, Controlled Unclassified Information (CUI) is an over-arching term that covers any information which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by government agencies as: For Official Use Only (FOUO) and any other identifier used by other government agencies to categorize information as CUI.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby attest that I am working on the **U.S. Navy, Fleet Readiness Center Southeast** construction project, meet the requirements of Construction Security Plan (CSP), and have a need-to-know for access to information related to this construction project.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me, and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

4. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific categories of information to which I am granted access. I understand that the United States Government may

conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

5. If I represent the prime contractor, I will have my subcontractor(s) and my suppliers complete and sign Appendix A, Controlled Unclassified Information Non-Disclosure Agreement PRIOR to releasing any copies or reproduction of any part of the solicitation documents. As the prime contractor I will keep a list of subcontractor(s) and suppliers who were provided the solicitation documents. I hereby agree that the Government reserves right to ask the list of subcontractor(s) and suppliers who were provided a copy of the solicitation documents.

6. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with all dissemination restrictions cited or verbally relayed to me by the proper authority.

7. I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access, or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to the United States Government; and/or 3) upon the determination that my official duties do not require further access to such information.

8. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may encounter unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products and will protect them in the same matter as the original.

9. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

10. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

11. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

12. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any CUI to which I have been given conditional access under the terms of this Agreement.

13. I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and always thereafter.

14. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

15. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

16. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

Name:	
Signature:	
Date:	
Company / Organization Name:	
Company / Organization Address:	
Company / Organization Phone Number:	
Witnessed By Name:	
Witnessed Date:	
Witness Organization:	

APPENDIX B: STATEMENT OF AFFILIATION

APPENDIX G: CRITICAL PROGRAM INFORMATION LIST

(U) Critical Information is specific, observable facts, generally unclassified, about friendly (e.g., U.S.) intentions, capabilities, or activities needed by adversaries for them to plan and act effectively against friendly objectives. Although "generally unclassified" in accordance with the ADIL classification guidance, in some circumstances this information may be classified.

(U) Provided below is a draft Critical Information with Indicators List (CIIL) for the project. It has been broken down into several stages to make the overall OPSEC effort easier to address and more manageable. The suggested stage and their associated suggested critical information are:

(U) **Architectural and Engineering Critical Information List**

- Requirements for facility (square footage, power, water, expected # of occupants)
- Conceptual designs/drawings
- Accepted designs/drawings
- Blueprints
- IT, Communications, Electrical, Plumbing, HVAC, wastewater, plans
- Redundant and backup systems and associated connections or cables
- Meeting notes
- Change orders and proposed modifications to plans
- Physical Security, Antiterrorism and Force Protection (ATFP), and Technical Security plans and requirements
- Communication methods (unprotected email, fax, telephone, etc.)
- Construction timelines
- Any unique features of the facility
- Location of sensitive areas within the facility and how they are identified
- Storage locations and methods for designs/drawings

(U) **Construction material procurement Critical Information List**

- Types of material
- Material selection methods
- Quantity of material
- Material inspection methods
- Origin/supplier of material
- Shipping, handling, storage methods and procedures
- Procurement methods

(U) **Transportation of construction materials Critical Information List**

- Contents of shipments
- Number of shipments and quantities within each shipment
- Paperwork for each shipment (inventory, POCs, costs, etc.)
- Origin of shipments
- Dates when shipment will be in transit
- Storage locations
- Route of shipment
- Security measures in shipments
- Communication methods

APPENDIX G (CONTINUED)

(U) **Structure Construction Critical Information**

- Blueprints/design documents
- Construction methods (if unique) or differ from general construction methods
- Security requirements and plans and procedures
- Schedule

(U) **Office Fit-Up Critical Information**

- Blueprints/design documents
- Schedule
- Location of cable trays, and plans and procedures during this phase
- Security requirements
- Telephone runs, power runs, and plans and procedures during this phase
- Other internal infrastructure

(U) **Office equipment/furniture procurement Critical Information**

- Types and quantity of equipment
- Procurement methods
- Equipment vendors and suppliers
- Shipping methods
- Schedule

(U) **Shipping of office equipment/furniture Critical Information**

- Contents of shipments
- Route of shipment
- Number of shipments and quantities within each shipment
- Storage locations
- Specific shipping methods
- Origin of shipments
- Procurement methods
- Dates when shipment will be in transit
- Security measures in shipments

(U) **Move of existing office equipment/furniture from other locations Critical Information**

- Existence of sensitive or specialized equipment
- Move schedule for sensitive equipment
- Communication methods

ANNEX E: PROPOSED SSA AND CONSTRUCTION LAYDOWN AREAS

Insert photo/drawing for laydown

ANNEX F: CHANGE OF RECORD

1. (U) This annex is provided to input changes, assessments, and memorandums for record. All attachments will be added by the SSM and dictated by the SAO's.

CH#	Subject	Change	Date
0	Initial release	v. 1.0	18 Oct 2024
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

ANNEX S: SIGNATURE BLOCK

1. FRCSE Site Security Manager
   David Steiner, SPSC, PSC, SFPC

2. FRCSE Legal Office

3. FRCSE Contracting Office

4. FRCSE Government Program Manager
   Savanna Masey

3. COMFRC Government SAP Security Officer
   Robert Purdy, SAPPC, Security+

4. NAVFAC SE Security Director

5. NAVFAC Project Manager

6. F-35 LIGHTING II Program Office Accreditation Officer